The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
ASPPortal 3.1.1	A vulnerability has been reported in ASPPortal that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	ASPPortal SQL Injection CVE-2006-1353	7	Secunia, Advisory: SA19286, March 21, 2006
Atrium Software Mercur Messaging Standard 5.0 SP3, Lite 5.0 SP3, Enterprise 5.0 SP3	A buffer overflow vulnerability has been reported in Mercur Messaging that could let remote malicious users cause a Denial of Service or arbitrary code execution. No workaround or patch	Mercur Messaging Denial of Service or Arbitrary Code Execution CVE-2006-1255	7	Secunia, Advisory: SA19267, March 17, 2006

	available at time of publishing. Proof of Concept exploit scripts, mercur.cpp and Mercur-5.0.c, have been published.			
avast! Antivirus Professional 4.6.763, Home	A vulnerability has been reported in avast! Antivirus, insecure default permissions, that could let local malicious users bypass security restrictions. No workaround or patch available at time of publishing. There is no exploit code required.	avast! Antivirus Security Restriction Bypassing CVE-2006-1355	7	Secunia, Advisory: SA19284, March 20, 2006
betaparticle blog 6.0 and prior	A input validation vulnerability has been reported in betaparticle blog that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	betaparticle blog SQL Injection CVE-2006-1333	4.7	Security Tracker, Alert ID: 1015788, March 20, 2006
MailEnable Standard Edition 1.91 and 1.92, Professional Edition 1.72 and prior, Enterprise Edition 1.2	Multiple buffer overflow vulnerabilities have been reported in MailEnable, Webmail and POP3, that could let remote malicious user cause a Denial of Service or execute arbitrary code. MailEnable There is no exploit code required.	MailEnable Denial of Service or Arbitrary Code Execution CVE-2006-1337 CVE-2006-1338	7 (CVE-2006-1337) 2.3 (CVE-2006-1338)	Secunia, Advisory: SA19288, March 20, 2006
Microsoft ASP.Net 1.1 SP1 and prior	A vulnerability has been reported in ASP.Net that could let remote malicious users cause a Denial of Service. Microsoft Microsoft A Proof of Concept exploit script, w3wp-dos.c, has been published.	Microsoft ASP.NET Denial of Service CVE-2006-1364	Not Available	Security Focus, ID: 17188, March 22, 2006
Microsoft Commerce Server 2002 before SP2	A vulnerability has been reported in Commerce Server 2002 that could let remote malicious users bypass security restrictions. Microsoft Commerce Server 2002 SP2 Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Commerce Server 2002 Security Restriction Bypassing CVE-2006-1257	7	Security Focus, ID: 17134, March 16, 2006
Microsoft Internet Explorer 6.0, 6.0 SP1, 6.0 SP2	An unspecified vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code, HTA applications. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Internet Explorer Arbitrary Code Execution	Not Available	Security Tracker, Alert ID: 1015800, March 21, 2006

Microsoft Internet Explorer 6.0.2900.2180	A buffer overflow vulnerability has been reported in Internet Explorer that could let remote malicious users cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Microsoft Internet Explorer Denial of Service CVE-2006-1245	7	Security Focus, ID: 17131, March 16, 2006
Microsoft Microsoft Office 2000, 2003 Professional, 2003 Small Business, 2003 Standard, 2003 Student, 2003 Student and Teacher, 2004 for Mac, X for Mac, XP Microsoft Works Suite 2001 to 2006 Microsoft Excel, Excel Viewer, Outlook, PowerPoint and Word various versions	Multiple vulnerabilities have been reported in Microsoft Office that could let remote malicious users execute arbitrary code. Microsoft Avaya **Nortell** **Version 1.2: Updated mitigations and work around section as well as the FAQ.** Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Office Multiple Arbitrary Code Execution CVE-2005-4131 CVE-2006-0009 CVE-2006-0028 CVE-2006-0029 CVE-2006-0030 CVE-2006-0031	2.8 (CVE-2005-4131) 5.6 (CVE-2006-0009) 5.6 (CVE-2006-0028) 5.6 (CVE-2006-0029) 5.6 (CVE-2006-0030) 5.6 (CVE-2006-0031)	Microsoft, Security Bulletin MS06-012, March 14, 2006 Cyber Security Alert SA06-073A Technical Cyber Security Alert TA06-073A US-CERT VU#339878, VU#235774, VU#123222, VU#642428, VU#104302, VU#682820 **Nortel, Bulletin 2006006777, March 17, 2006** **Microsoft, Security Bulletin MS06-012 v1.2, March 17, 2006**
Microsoft Windows IGMPv3 XP and Server 2003 various versions	A vulnerability has been reported in Windows IGMPv3 that could let remote malicious users cause a Denial of Service. Microsoft **Version 1.2: Updated to reflect that this update does not supersede MS05-019 for Windows Server 2003 SP1.** There is no exploit code required.	Microsoft Windows IGMPv3 Denial of Service CVE-2006-0021	**2.3**	Microsoft, Security Bulletin MS06-007 V1.1, February 14, 2006 **Microsoft, Security Bulletin MS06-007 V1.2, March 17, 2006**
Microsoft Windows XP SP1, Server 2003, and Server 2003 for Itanium Systems	A vulnerability has been reported in Windows, default ACL settings, that could let remote malicious users obtain elevated privileges. Microsoft Avaya **Version 1.1: Updated to reflect the appropriate registry key for file detection on Windows Server 2003.** There is no exploit code required.	Microsoft Windows Privilege Elevation CVE-2006-0023	2.9	Microsoft, Security Bulletin MS06-011, March 14, 2006 **Microsoft, Security Bulletin MS06-011 V1.1, March 17, 2006**
TrendMicro PC-cillin Internet Security 14.00.1485, 14.10.0.1023	A vulnerability has been reported in PC-cillin Internet Security, insecure default directory permissions, that could let local malicious users obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	PC-cillin Internet Security Privilege Elevation	Not Available	Secunia, Advisory: SA19282, March 22, 2006

Veritas Backup Exec for Windows Servers 9.1, 10.0, 10.1	A vulnerability has been reported in Backup Exec for Windows Servers that could let remote malicious users cause a Denial of Service or arbitrary code execution. Veritas 282254, 282279, 282255 Currently we are not aware of any exploits for these vulnerabilities.	Veritas Backup Exec for Windows Servers Denial of Service or Arbitrary Code Execution CVE-2006-1297 CVE-2006-1298	2.3 (CVE-2006-1297) 3.4 (CVE-2006-1298)	Security Tracker, Alert ID: 1015785, March 17, 2006
Virtual Communication Services VPMi 3.3	A vulnerability has been reported in VPMi 3.3 that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	VPMi Cross-Site Scripting CVE-2006-1266	2.3	Security Focus, ID: 17172, March 21, 2006
WinHKI 1.6	A directory traversal vulnerability has been reported in WinHKI, RAR, TAR, ZIP and TAR.GZ archive handling, that could let remote malicious users obtain unauthorized system access. No workaround or patch available at time of publishing. There is no exploit code required.	WinHKI Unauthorized System Access CVE-2006-1323	5.6	Secunia, Advisory: SA19296, March 20, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Apple Mac OS X Server 10.4-10.4.5, Mac OS X 10.4-10.4.5	Multiple vulnerabilities have been reported: a vulnerability was reported in JavaScript because in certain circumstances because it is possible to bypass the same-origin policy; a buffer overflow vulnerability was reported in Mail due to a boundary error, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in Safari/LaunchServices due to an error which could lead to the execution of a malicious file. Updates available Currently we are not aware of any exploits for these vulnerabilities.	Mac OS X Security Update CVE-2006-0396 CVE-2006-0397 CVE-2006-0398 CVE-2006-0399 CVE-2006-0400	**5.6** (CVE-2006-0396) 5.6 (CVE-2006-0397) 5.6 (CVE-2006-0398) 5.6 (CVE-2006-0399) 7 (CVE-2006-0400)	Apple Security Update, APPLE-SA-2006-03-13, March 13, 2006 **US-CERT VU#980084**
Beagle Beagle 0.2.2.1.	A vulnerability has been reported in the 'beagle-status' script because the 'beagle-info' script runs insecurely, which could let a malicious user execute arbitrary commands. Fedora Currently we are not aware of any exploits for this vulnerability.	Beagle 'beagle-status' Command Execution CVE-2006-1296	7	Secunia Advisory: SA19278, March 17, 2006 Fedora Update Notification, FEDORA-2006-188, March 21, 2006
Crossfire Crossfire 1.9 , 1.8	A buffer overflow vulnerability has been reported in 'request.c' due to an error in the 'SetUp()' function when handling the 'setup' command, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. **Debian** A Proof of Concept exploit script,	CrossFire Remote Buffer Overflow CVE-2006-1236	7	Secunia Advisory: SA19237, March 14, 2006 **Debian Security Advisory, DSA-1009-1, March 20, 2006**

	crossfire_bof_exp.c, has been published.			
Daniel Stenberg curl 7.12-7.15, 7.11.2	A buffer overflow vulnerability has been reported due to insufficient bounds checks on user-supplied data before using in a finite sized buffer, which could let a local/remote malicious user execute arbitrary code. Upgrades available Mandriva Fedora Debian Fedora OpenPKG Gentoo RedHat **OpenOffice** Currently we are not aware of any exploits for this vulnerability.	cURL / libcURL URL Parser Buffer Overflow CVE-2005-4077	4.9	Security Focus, Bugtraq ID: 15756, December 7, 2005 Mandriva Linux Security Advisory, MDKSA-2005:224, December 8, 2005 Fedora Update Notifications, FEDORA-2005-1129 & 1130, December 8, 2005 Debian Security Advisory, DSA 919-1, December 12, 2005 Fedora Update Notifications FEDORA-2005-1136 & 1137, December 12, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.028, December 12, 2005 Gentoo Linux Security Advisory, GLSA 200512-09, December 16, 2005 RedHat Security Advisory, RHSA-2005:875-4, December 20, 2005 **Secunia Advisory: SA19261, March 16, 2006**
Debian Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A vulnerability has been reported in 'log.c' due to the insecure creation of the log file, which could let a remote malicious user overwrite sensitive data or configuration files. Debian There is no exploit code required.	SNMPTRAPFMT Insecure Temporary File Creation CVE-2006-0050	Not Available	Debian Security Advisory DSA-1013-1, March 22, 2006
Debian libcgi-session-perl 4.03-1	Multiple vulnerabilities have been reported in the libcgi-session-perl package due to the insecure creation of temporary files, which could let a remote/local malicious user overwrite files or obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Libcgi-session-perl Insecure Temporary File Creation	Not Available	Security Focus, Bugtraq ID: 17177, March 21, 2006
Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	An information disclosure vulnerability has been reported because sensitive information is improperly stored in world-readable files, which could let a malicious user obtain sensitive information. The vulnerability will reportedly be fixed in version 4.0.14-9 of the shadow package. There is no exploit code required.	Debian GNU/Linux Information Disclosure	Not Available	Security Focus, Bugtraq ID: 17122, March 15, 2006
Free RADIUS FreeRADIUS 1.0-1.0.5	A vulnerability has been reported in the EAP-MSCHAPv2 state machine due to an error, which could let a malicious user bypass authentication and cause a Denial of Service. Updates available Currently we are not aware of any	FreeRADIUS EAP-MSCHAPv2 Authentication Bypass CVE-2006-1354	8	Security Focus, Bugtraq ID: 17171, March 21, 2006

	exploits for this vulnerability.			
FreeBSD FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.4 -PRERELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, 5.2 -RELENG, -RELEASE, 5.2, 5.1 -RELENG, 5.1 -RELEASE/Alpha, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.0 -RELENG, 5.0 -RELEASE-p14, 5.0 alpha, 5.0, 4.11 -STABLE, 4.11 -RELENG, 4.11 -RELEASE-p3, 4.10 -RELENG, 4.10 -RELEASE-p8, 4.10 -RELEASE, 4.10, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 5.4-STABLE, 4.10-PRERELEASE	A vulnerability has been reported in the IPsec implementation due to the improper handling of sequence numbers, which could let a remote malicious user replay IPsec traffic. Patches available Currently we are not aware of any exploits for this vulnerability.	FreeBSD IPsec Replay CVE-2006-0905	Not Available	FreeBSD Security Advisory, FreeBSD-SA-06:11, March 22, 2006
FreeBSD All FreeBSD releases	A vulnerability has been reported in OPIE, which could let a remote malicious user change passwords for arbitrary accounts. Patches available There is no exploit code required.	OPIE Arbitrary Account Password Change CVE-2006-1283	Not Available	FreeBSD Security Advisory, FreeBSD-SA-06:12, March 22, 2006
GlFtpd glFTPd prior to 2.01 RC5	A vulnerability has been reported in the IP address checking due to an error, which could let a remote malicious user bypass certain security restrictions. Updates available Vulnerability can be exploited through use of a FTP client.	GLFTPD IP Check Security Bypass CVE-2006-1253	7	Secunia Advisory: SA19221, March 15, 2006
GNOME Development Team Evolution 2.3.1-2.3.7	A buffer overflow vulnerability has been reported which could lead to a Denial of Service when processing messages that contain inline XML file attachments with excessively long strings. **Mandriva** Currently we are not aware of any exploits for this vulnerability.	GNOME Evolution Remote Buffer Overflow CVE-2006-0528	**2.3**	Security Focus, Bugtraq ID: 16408, January 30, 2006 **Mandriva Linux Security Advisory, MDKSA-2006:057, March 20, 2006**
GNU GNU Privacy Guard prior to 1.4.2.2.	A vulnerability has been reported caused due to an error in the detection of unsigned data, which could let a remote malicious user inject arbitrary data and bypass verification. Updates available Debian Gentoo Fedora SuSE Slackware RedHat **Ubuntu** **Trustix** There is no exploit code required.	GnuPG Unsigned Data Injection Detection CVE-2006-0049	2.3	GNU Security Advisory, March 9, 2006 Debian Security Advisory, DSA 993-1, March 10, 2006 Gentoo Linux Security Advisory, GLSA 200603-08, March 10, 2006 SUSE Security Announcement, SUSE-SA:2006:014, March 10, 2006 Slackware Security Advisory, SSA:2006-072-02, March 13, 2006 RedHat Security Advisory, RHSA-2006:0266-8, March 15, 2006 **Ubuntu Security Notice, USN-264-1, March 13, 2006** **Trustix Secure Linux Security Advisory #2006-0014, March 20, 2006**

Hewlett Packard Company HP-UX B.11.23, B.11.11, B.11.00	A vulnerability has been reported in the 'usermod' command when handling the '-u' and '-m' commandline options, which could let a malicious user obtain unauthorized access. Patches available Currently we are not aware of any exploits for this vulnerability.	HP-UX Usermod Unauthorized Access CVE-2006-1248	4.9	HP Security Bulletin, HPSBUX02102, March 17, 2006
IBM AIX 5.3	An unspecified security vulnerability has been reported in the 'mklvcopy' command. The impact was not specified. IBM has released an APAR to address this issue. Currently we are not aware of any exploits for this vulnerability.	IBM AIX 'mklvcopy' Security Vulnerability CVE-2006-1246	4.9	Security Focus, Bugtraq ID: 17115, March 16, 2006
IlohaMail IlohaMail 0.7 .0-0.7.9, 0.8.6-0.8.14	Cross-Site Scripting vulnerabilities have been reported when processing emails due to an input validation error, which could let a remote malicious user execute arbitrary HTML and script code. **Debian** There is no exploit code required.	IlohaMail Email Message Remote Cross-Site Scripting CVE-2005-1120	3.3	Secunia Advisory, April 14, 2005 **Debian Security Advisory, DSA-1010-1, March 20, 2006**
Jabber Software Foundation Jabber Server 2.0 s8-s10, 2.0	A remote Denial of Service vulnerability has been reported due to a failure of the application to properly handle malformed network messages. Updates available Vulnerability can be exploited through the use of a client application for jabber.	Jabber Studio JabberD Remote Denial of Service CVE-2006-1329	2.3	Security Focus, Bugtraq ID: 17155, March 20, 2006
Lincoln D. Stein Crypt::CBC 2.16 & prior	A vulnerability has been reported due to a flaw in its creation of IVs (Initialization Vectors) for ciphers with a blocksize larger than 8 when the RandonIV-style header is used, which could let a remote malicious user bypass security restrictions. Updates available Debian **Gentoo** Currently we are not aware of any exploits for this vulnerability.	Lincoln D. Stein Crypt::CBC Perl Module Weak Ciphertext Security Bypass CVE-2006-0898	1.3	Secunia Advisory: SA18755, February 27, 2006 Debian Security Advisory, DSA-996-1, March 13, 2006 **Gentoo Linux Security Advisory, GLSA 200603-15, March 17, 2006**
Metamail Metamail 2.7	A buffer overflow vulnerability has been reported when handling boundary headers within email messages, which could let a remote malicious user execute arbitrary code. *Note: According to Security Tracker this is a Linux/Unix vulnerability. Previously classified as multiple operating systems.* RedHat Mandriva SuSE Debian **Gentoo** A Proof of Concept exploit has been published.	Metamail Remote Buffer Overflow CVE-2006-0709	7	Security Focus, Bugtraq ID: 16611, February 13, 2006 RedHat Security Advisory, RHSA-2006:0217-4, February 21, 2006 Mandriva Security Advisory, MDKSA-2006:047, February 22, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 Debian Security Advisory, DSA-995-1, March 13, 2006 **Gentoo Linux Security Advisory, GLSA 200603-16, March 17,**

				2006
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE3-STABLE10, STABLE1	A remote Denial of Service vulnerability has been reported when handling certain client NTLM authentication request sequences. Upgrades available Ubuntu Debian Mandriva SCO SUSE RedHat **RHSA-2006:0045-8** Currently we are not aware of any exploits for this vulnerability.	Squid NTLM Authentication Remote Denial of Service CVE-2005-2917	3.3	Secunia Advisory: SA16992, September 30, 2005 Ubuntu Security Notice, USN-192-1, September 30, 2005 Debian Security Advisory, DSA 828-1, September 30, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:181, October 11, 2005 SCO Security Advisory, SCOSA-2005.44, November 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 RedHat Security Advisory, RHSA-2006:0052-7, March 7, 2006 **RedHat Security Advisory, RHSA-2006:0045-8, March 15, 2006**

Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib Debian Ubuntu OpenBSD Mandriva Fedora Slackware FreeBSD SUSE Gentoo Gentoo Trustix Conectiva Apple TurboLinux SCO Debian Trolltech FedoraLegacy Debian Mandriva Ubuntu Ubuntu SCO **glsa-200603-18** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CVE-2005-1849	3.3	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announce-ment, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory, TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14340, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Debian Security Advisory, DSA 797-2, September 29, 2005 Mandriva Linux Security Advisory, MDKSA-2005:196, October 26, 2005 Ubuntu Security Notice, USN-151-3, October 28,

				2005 Ubuntu Security Notice, USN-151-4, November 09, 2005 SCO Security Advisory, SCOSA-2006.6, January 10, 2006 **Gentoo Linux Security Advisory, GLSA 200603-18, March 21, 2006**
Multiple Vendors Gerrit Pape runit 1.4, 1.3.x, 1.2.x, 1.0.x, 0.x; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in 'uidgid.h' due to an integer type definition error, which could let a remote/local malicious user obtain elevated privileges. Runit There is no exploit code required.	RunIt CHPST Elevated Privileges CVE-2006-1319	5.6	Security Focus, Bugtraq ID: 17179, March 21, 2006
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A vulnerability has been reported in the EXT2/EXT3 file systems, which could let a remote malicious user bypass access controls. Ubuntu Mandriva RedHat Mandriva Debian **RHSA-2006-0144** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2/EXT3 File Access Bypass CVE-2005-2801	3.3	Security Focus, Bugtraq ID: 14792, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 Mandriva Linux Security Advisory, MDKSA-2005:219, November 30, 2005 Debian Security Advisory, DSA 921-1, December 14, 2005 **RedHat Security Advisory, RHSA-2006-0144, March 16, 2006**
Multiple Vendors Linux kernel 2.6-2.6.16	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in the 'do_replace()' function in Netfilter, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability was reported in 'drivers/usb/gadget/mdis.c' when handling a NDIS response to 'OID_GEN_SUPPORTED _LIST,' which could lead to the corruption of kernel memory. Updates available Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Buffer Overflows CVE-2006-0038	Not Available	Secunia Advisory: SA19330, March 22, 2006
Multiple Vendors Mail-Audit 2.1, 2.0; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha, 3.0	A vulnerability has been reported due to the insecure creation of temporary files when logging is enabled, which could let a malicious user cause a Denial of Service or overwrite files. Debian **DSA 960-3** There is no exploit code required.	Mail-Audit Insecure Temporary File Creation CVE-2005-4536	**1.6**	Debian Security Advisory, DSA-960-1, January 31, 2006 **Debian Security Advisory, DSA 960-3, March 20, 2006**

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Trustix Secure Linux 3.0, 2.2, Trustix Secure Enterprise Linux 2.0; SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9; Linux kernel 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions. Linux Kernel Ubuntu SUSE Trustix Mandriva Mandriva: SUSE: Conectiva RedHat RedHat **RHSA-2006-0144** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Invalid Memory Access Denial of Service CVE-2005-2458	3.3	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006 **RedHat Security Advisory, RHSA-2006-0144, March 16, 2006**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Linux kernel 2.6-2.6.12 .3	An information disclosure vulnerability has been reported in 'SYS_GET_THREAD _AREA,' which could let a malicious user obtain sensitive information. Kernel versions 2.6.12.4 and 2.6.13 are not affected by this issue. Ubuntu Mandriva Debian Conectiva RedHat **RHSA-2006-0144** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Information Disclosure CVE-2005-3276	2.3	Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 Debian Security Advisory, DSA 922-1, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 **RedHat Security Advisory, RHSA-2006-0144, March 16, 2006**
Multiple Vendors X.org 1.0.0 & later, X11R6.9.0, X11R7.0 ; Sun Solaris 10.0 _x86; SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS; RedHat Fedora Core5; MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0	A vulnerability has been reported due to an error when checking a user's privileges because the address of the 'geteuid()' function is tested and not the result of the function, which could let a malicious user bypass security restrictions. Patches available Fedora Mandriva Sun SuSE An exploit script, xmodulepath.tgz,	X.Org X Window Server Security Restriction Bypass CVE-2006-0745	7	Security Focus, Bugtraq ID: 17169, March 20, 2006 Sun(sm) Alert Notification Sun Alert ID: 102252, March 20, 2006 Mandriva Linux Security Advisory, MDKSA-2006:056, March 20, 2006 SUSE Security Announcement, SUSE-SA:2006:016, March 21, 2006

	has been published.			
Multiple Vendors Zoo 2.10; Gentoo Linux	A buffer overflow vulnerability has been reported in 'parse.c' due to a boundary error in the 'parse' function when creating an archive from a file with an overly long pathname, which could let a malicious user execute arbitrary code. Gentoo A Proof of Concept exploit has been published.	Zoo Buffer Overflow CVE-2006-1269	5.6	Secunia Advisory: SA19250, March 16, 2006
Paul Vixie Vixie Cron 4.1	A vulnerability has been reported due to insecure creation of temporary files when crontab is executed with the '-e' option, which could let a malicious user obtain sensitive information. Fedora RedHat **RHSA-2006:0117-7** There is no exploit code required; however, a Proof of Concept exploit script has been published.	Vixie Cron Crontab Information Disclosure CVE-2005-1038	2.3	Security Focus, 13024, April 6, 2005 Fedora Update Notification, FEDORA-2005-320, April 15, 2005 Fedora Update Notifications, FEDORA-2005-550 & 551, July 12, 2005 RedHat Security Advisory, RHSA-2005:361-19, October 5, 2005 **RedHat Security Advisory, RHSA-2006:0117-7, March 15, 2006**
PEAR PEAR::Auth 1.2.4 & prior to 1.3.0r4	Multiple unspecified SQL injection vulnerabilities have been reported due to insufficient sanitization , which could let a remote malicious user execute arbitrary SQL code. Updates available **Gentoo** There is no exploit code required.	PEAR::Auth Multiple Unspecified SQL Injection **CVE-2006-0868**	**7**	Security Focus, Bugtraq ID: 16758, February 21, 2006 **Gentoo Linux Security Advisory, GLSA 200603-13, March 17, 2006**
Royal Institute of Technology Heimdal prior to 0.6.6 & 0.7.2	A vulnerability has been reported in the 'rshd' server when storing forwarded credentials due to an unspecified error, which could let a malicious user obtain elevated privileges. Update to version 0.7.2 or 0.6.6. Ubuntu Debian SuSE **Gentoo** Currently we are not aware of any exploits for this vulnerability.	Heimdal RSHD Server Elevated Privileges CVE-2006-0582	1.6	Security Tracker Alert ID: 1015591, February 7, 2006 Ubuntu Security Notice, USN-247-1, February 09, 2006 Debian Security Advisory, DSA-977-1, February 16, 2006 SUSE Security Announcement, SUSE-SA:2006:011, February 24, 2006 **Gentoo Linux Security Advisory, GLSA 200603-14, March 17, 2006**
Sendmail Consortium Sendmail prior to 8.13.6	A vulnerability has been reported due to a race condition caused by the improper handling of asynchronous signals, which could let a remote malicious user execute arbitrary code. Updates available Currently we are not aware of any exploits for these vulnerabilities.	Sendmail Asynchronous Signal Handling Remote Code Execution CVE-2006-0058	Not Available	Internet Security Systems Protection Advisory, March 22, 2006 Technical Cyber Security Alert TA06-081A US-CERT VU#834865
TEG Tenes Empanadas Graciela 0.11.1	A remote Denial of Service vulnerability has been reported due to an off-by-one error within the handling of the nickname supplied by	Tenes Empanadas Graciela Remote Denial of Service	**3.3**	Security Focus, Bugtraq ID: 16982, March 6, 2006 **Security Focus, Bugtraq**

	the user. **Patch available** Vulnerability can be exploited through use of a client version of the application.	**CVE-2006-1150**		**ID: 16982, March 21, 2006**
util-vserver util-vserver 0.x	A vulnerability has been reported because the default policy is set to trust all unknown capabilities instead of considering them as insecure, which could potentially let a malicious user bypass security restrictions. Updates available Debian Currently we are not aware of any exploits for this vulnerability.	util-vserver Unknown Capabilities Handling CVE-2005-4418	Not Available	Debian Security Advisory DSA-1011-1, March 21, 2006
XPVM XPVM 1.2.5	An insecure file creation vulnerability has been reported in XPVM that could let local malicious users arbitrarily overwrite files. **Debian** There is no exploit code required.	XPVM Arbitrary File Overwrite CVE-2005-2240	2.3	Secunia Advisory: SA16040, July 12, 2005 **Debian Security Advisory, DSA-1003-1, March 16, 2006**

[back to top]

Multiple Operating Systems - Windows/UNIX/Linux/Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
1Web Calendar 1WebCalendar 4.0	SQL injection vulnerabilities have been reported in 'viewEvent.cfm' due to insufficient sanitization of the 'EventID' parameter, in 'news/newsView.cfm' due to insufficient sanitization of the 'NewsID' parameter, and in 'mainCal.cfm' due to insufficient sanitization of the 'ThisDate' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited using a web client; however, a Proof of Concept exploit has been published.	1WebCalendar SQL Injection	Not Available	Secunia Advisory: SA19329, March 22, 2006
Adobe Flash Player 8.0.22.0 and prior, Breeze Meeting Add-In 5.1 and prior, Shockwave Player 10.1.0.11 and prior, Flash Debug Player 7.0.14.0 and prior	A vulnerability has been reported in Flash Player that could let remote malicious users execute arbitrary code. Adobe (formerly Macromedia) **RedHat** **SuSE** **Gentoo** Currently we are not aware of any exploits for these vulnerabilities.	Flash Player Arbitrary Code Execution CVE-2006-0024	**5.6**	Adobe, Security Bulletin APSB06-03, March 14, 2006 **US-CERT VU#945060** **RedHat Security Advisory, RHSA-2006:0268-5, March 15, 2006** **SUSE Security Announcement, SUSE-SA:2006:015, March 21, 2006** **Gentoo Linux Security Advisory, GLSA-200603-20, March 21, 2006**
BEA Systems, Inc. WebLogic Express 6.x, 7.x, 8.x, WebLogic Server 6.x, 7.x, 8.x	Several vulnerabilities have been reported: a vulnerability was reported due to an error in the restriction of an unspecified internal servlet, which could let a remote malicious user with HTTP access obtain sensitive information; and a remote Denial of Service vulnerability was reported due to an error in the XML parser. Update information	BEA WebLogic Server/Express HTTP Splitting & Remote Denial of Service CVE-2006-1351 CVE-2006-1352	2.3 (CVE-2006-1351) 2.3 (CVE-2006-1352)	BEA Systems Security Advisories, BEA06-120.00 & BEA06-123.00, March 20, 2006

	Update information There is no exploit code required.			
BEA Systems, Inc. WebLogic Portal 8.1 , SP1-SP5, 8.0	A vulnerability has been reported in the JSR-168 Portlets because they are incorrectly rendered from the cache, which could let a remote malicious user obtain sensitive information. Patch information Vulnerability can be exploited through use of a client application.	BEA WebLogic Portal JSR-168 Portlets Information Disclosure CVE-2006-1358	2.3	BEA Systems Security Advisory, BEA06-122.00, March 20, 2006
Border Ware Technologies Inc. MXtreme 6.0, 5.0	A vulnerability has been reported due to an unspecified error in the web administration. The impact was not specified. Updates available Currently we are not aware of any exploits for this vulnerability.	BorderWare MXtreme Web Administration CVE-2006-1254	4.9	Security Tracker Alert ID: 1015787, March 17, 2006
Contrexx Contrexx 1.0.8, 1.0.7, 1.0.5, 1.0.4	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	Contrexx CMS Cross-Site Scripting CVE-2006-1293	2.3	Security Focus, Bugtraq ID: 17128, March 16, 2006
CutePHP Team CuteNews 1.4.1	A vulnerability has been reported due to insufficient sanitization of the 'archive' parameter in a POST request or in a cookie, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client.	CuteNews 'archive' Information Disclosure CVE-2006-1339 CVE-2006-1340	1.9 (CVE-2006-1339) 1.9 (CVE-2006-1340)	Secunia Advisory: SA19289, March 20, 2006
Daniel Stenberg curl 7.15-7.15.2	A buffer overflow vulnerability has been reported when parsing a URL that contains the TPTP protocol prefix 'tfpt://' due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Updates available Gentoo Fedora Currently we are not aware of any exploits for this vulnerability.	cURL / libcURL TFTP URL Parser Buffer Overflow CVE-2006-1061	7	Security Focus, Bugtraq ID: 17154, March 20, 2006 Gentoo Linux Security Advisory, GLSA 200603-19, March 21, 2006 Fedora Update Notification, FEDORA-2006-189, March 21, 2006
Drupal Drupal prior to 4.5.8 & 4.6.6	Multiple vulnerabilities have been reported: a vulnerability was reported when using 'menu.module' to create a menu item, which could let a remote malicious user bypass security restrictions; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported when handling sessions during login due to an error, which could let a remote malicious user hijack another user's session; and a vulnerability was reported due to insufficient sanitization of unspecified input before using in mail headers, which could let a remote malicious user inject arbitrary headers in outgoing mails. Updates available **Debian** Vulnerabilities can be exploited through a web client.	Drupal Multiple Vulnerabilities CVE-2006-1225 CVE-2006-1226 CVE-2006-1227 CVE-2006-1228	**2.3** (CVE-2006-1225) 2.3 (CVE-2006-1226) **4.9** (CVE-2006-1227) 5.6 (CVE-2006-1228)	Secunia Advisory: SA19245, March 14, 2006 **Debian Security Advisory, DSA-1007-1, March 17, 2006**

Ext Calendar ExtCalendar 1.0	Cross-Site Scripting vulnerabilities have been reported in 'calendar.php' due to insufficient sanitization of the 'month,' 'year,' 'prev,' and 'next' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. This issue is reportedly addressed in ExtCalendar 2.0. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	ExtCalendar Cross-Site Scripting CVE-2006-1336	7	Secunia Advisory: SA19321, March 21, 2006
F5 Software FirePass 4100 5.4.2 , FirePass	A Cross-Site Scripting vulnerability has been reported in 'my.support.php3' due to insufficient sanitization of the 's' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	F5 Firepass 4100 SSL VPN Cross-Site Scripting CVE-2006-1357	2.3	Security Focus, Bugtraq ID: 17175, March 21, 2006
FFmpeg FFmpeg 0.4.9 -pre1, 0.4.6-0.4.8, FFmpeg CVS	A buffer overflow vulnerability has been reported in the 'avcodec_default_get_buffer()' function of 'utils.c' due to a boundary error, which could let a remote malicious user execute arbitrary code. Patches available Ubuntu Mandriva Ubuntu Gentoo Gentoo Debian **DSA-1004-1** **DSA-1005-1** Currently we are not aware of any exploits for this vulnerability.	FFmpeg Remote Buffer Overflow CVE-2005-4048	7	Secunia Advisory: SA17892, December 6, 2005 Ubuntu Security Notice, USN-230-1, December 14, 2005 Mandriva Linux Security Advisories MDKSA-2005:228-232, December 15, 2005 Ubuntu Security Notice, USN-230-2, December 16, 2005 Gentoo Linux Security Advisory, GLSA 200602-01, February 5, 2006 Gentoo Linux Security Advisory, GLSA 200603-03, March 4, 2006 Debian Security Advisory, DSA-992-1, March 10, 2006 **Debian Security Advisories, DSA-1004-1 & DSA-1005-1, March 16, 2006**
Free Articles Directory Free Articles Directory	A file include vulnerability has been reported in 'index.php' due to insufficient verification of the 'page' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client.	Free Articles Directory Page Parameter Directory Remote File Include CVE-2006-1350	7	Secunia Advisory: SA19320, March 22, 2006
FreeWPS FreeWPS 2.11	A file upload vulnerability has been reported in 'ImageManager' script, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	FreeWPS 'ImageManager' File Upload CVE-2006-1363	Not Available	Secunia Advisory: SA19343, March 22, 2006
funkwerk Funkwerk X2300 Family	Several vulnerabilities have been reported which could potentially let a remote malicious user cause a Denial of Service and an unknown impact. Updates available There is no exploit code required.	Funkwerk X2300 ISAKMP IKE Message Processing CVE-2006-1268	3.3	Secunia Advisory: SA19233, March 15, 2006

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Motorola Cellular Phones Security Dialog Spoofing & Remote Denial of Service: Several vulnerabilities have been reported in Motorola PEBL U6 and Motorola V600, which can be exploited by malicious people to trick users into accepting certain security dialogs and cause a Denial of Service.
- Mobiles help knowledge workers most: According to a report from the Centre for Economic and Business Research (CEBR), mobile phones increased the productivity of workers by nearly one percent in 2004. According to the report, mobile phones enabled staff to save about 20 minutes per day. However, the research also found that benefits were largely concentrated in the hands of two million mobile knowledge workers. These tend to be professionals who make heavy use of mobiles to keep in touch with customers and colleagues while traveling.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Multiple Vulnerabilities in Adobe Macromedia Flash: US-CERT is aware of several vulnerabilities in Adobe Macromedia Flash products. A system may be compromised if a user accesses a web page that references a specially crafted Flash (SWF) file.
- FaceTime identifies new IM botnet threat: A new threat has been identified by research experts at FaceTime Security Labs(TM) that affects instant messaging (IM) applications. Acting on an anonymous tip, they uncovered two "botnet" networks that collectively represent up to 150,000 compromised computers. One is used as a vehicle to fraudulently scan desktop and back-end systems to obtain credit card numbers, bank accounts, and personal information including log-ins and passwords.
- Crimeware, Trojan redirector targeting more than 100 banks: Websense® Security Labs™ has received reports of a Trojan Horse that is targeting users of more than 100 financial institutions in the United States and Europe. The malicious code checks to see if there is an active window open (either "my computer" or Internet Explorer). If one of these applications is not open, the malicious code modifies the contents of the hosts file on the local machine with a list of sites all pointing to localhost (127.0.0.1). If either of these applications is open, the malicious code performs a DNS lookup to a DNS server hosted in Russia and receives an address for a website.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender’s address.
5	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
6	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
7	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.

8	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
9	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
10	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.

Table updated March 20, 2006

[back to top]

Last updated March 23, 2006